STATEWIDE INFORMATION TECHNOLOGY POLICY

Interim Policy: Enterprise Information Technology Security Policy

Effective Date: January 1, 2008 Individual sections of this policy specifying other effective milestones/timeframes shall be in effect at those milestone/timeframes.

Approved:

Replaces & Supercedes: This policy may conflict with parts of other statewide information technology (IT) policies currently in effect. Where conflicts exist, the more restrictive policy shall take precedence.

I. Purpose

The purpose of this Enterprise Information Technology Security Policy is to define a set of minimum security requirements that all statewide entities (SE) shall meet in the statewide information technology (IT) context.

The primary objectives of this IT Security Policy are to:

- Define the effective management of the risk of security exposure or compromise within SE systems;
- communicate the responsibilities for the protection of SE information;
- establish a secure processing base and a stable processing environment;
- reduce the opportunity for errors to be entered into an electronic system supporting SE business processes;
- preserve management's options in the event of an information asset misuse, loss or unauthorized disclosure;
- promote and increase the awareness of information technology security in all SEs.

The intent of this policy is to specify requirements based upon industry best practices and to promote a framework that adheres to existing Federal statues and policy pertaining to confidentiality, privacy, accessibility, availability, and integrity.

This policy is a statement of the minimum requirements and roles and responsibilities required to establish and maintain a secure environment, and achieve the state’s information technology security objectives. Any SE may exceed the security requirements established in this document, but must at a minimum achieve the security levels required by this policy.

II. Applicability

This policy is applicable to statewide entities, staff and all others, including outsourced third parties, which have access, use or manage SE information assets in a statewide information technology (IT) context. Where conflicts exist between this policy and a SE's policy, the more restrictive policy shall take precedence.

This policy encompasses information technology (IT) systems, automated and manual, for which the state has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. It addresses information in the statewide information technology context, regardless of the form or format, which is created or used in support of business activities of statewide entities. This policy shall be communicated to staff and others who have access to or manage SE information.

III. Implementation Timetable

Policy requirements shall be implemented not later than the beginning of the State of Montana fiscal year, as stipulated in Table 1. Policy content not accompanied with an explicit implementation milestone/date shall be implemented not later than the Policy Effective Date.

Requirement	Timeframe
Information-Related Requirements	FY2010
Organizational IT Security Requirements	FY2010
Information Protection and Control Requirements	FY2010
Personnel Security Requirements	FY2009
Physical and Environmental Security Requirements	FY2010
Communications and Network Management Requirements	FY2011
Operational Management Requirements	FY2010
Access Control Requirements	FY2011
Systems Development and Maintenance Requirements	FY2010
Monitoring, Compliance and Enforcement Requirements	FY2009

Table 1 - Implementation Timetable

IV. Definition(s)

Refer to the Statewide Information Technology Policies and Standards Glossary for a complete list of definitions.

Authentication: The process to establish and prove the validity of a claimed identity.

Authenticity: This is the exchange of security information to verify the claimed identity of a communications partner.

Authorization: The granting of rights, which includes the granting of access based on an authenticated identity.

Availability: This is the 'property' of being operational, accessible, functional and usable upon demand by an authorized entity, e.g. a system or user

Business Risk: In the context of this policy, this is the combination of sensitivity, threat and vulnerability.

Computer: All physical, electronic and other components, types and uses of computers, including but not limited to hardware, software, central processing units, electronic communications and systems, databases, memory, Internet service, information systems, laptops, Personal Digital Assistants and accompanying equipment used to0 support the use of computers, such as printers, fax machines and copiers, and any updates, revisions, upgrades or replacements thereto.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls: Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

Cracking: Breaking into or attempting to break into another system in excess of one's access rights or authorization with or without malicious intent.

Critical: A condition, vulnerability or threat that could cause danger to data, a system, network, or a component thereof.

Custodian of Information: An employee or organizational unit acting as a caretaker of an automated file or database on behalf of its owner.

Data: Any information created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media. Data may include, but is not limited to personally identifying information, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Data Security: The protection of information assets from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that information.

Decryption: The reversal of a corresponding reversible encryption to render information intelligible using the appropriate algorithm and key.

Denial of Service: An attack that takes up so much of the company's business resource that it results in degradation of performance or loss of access to the company's business services or resources.

DMZ: Demilitarized zone; a semi-secured buffer or region between two networks such as between the public Internet and the trusted private State network.

Encryption: The cryptographic transformation of data to render it unintelligible through an algorithmic process using a cryptographic key.

Firewall: A security mechanism that creates a barrier between networks.

Host: A system or computer that contains business and/or operational software and/or data.

Incident: Any adverse event that threatens the confidentiality, integrity or accessibility of information resources.

Incident Response: The manual and automated procedures used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Information: Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Information Assets: (1) All categories of automated information, including but not limited to: records, files, and databases, and (2) information technology facilities, equipment (including microcomputer systems), and software owned or leased by the State.

Information Owner: An individual or a group of individuals that has responsibility for making protection and control decisions regarding use of information.

Information technology security: The concepts, techniques and measures used to protect information from accidental or intentional unauthorized access, modification, destruction, disclosure or temporary or permanent loss (See Availability).

Information technology security Architecture: A framework designed to ensure information technology security Principles are defined and integrated into business and IT processes in a consistent manner.

Integrity: The property that data has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Intrusion Detection: The monitoring of network activities, primarily through automated measures, to detect, log and report upon actual or suspected authorized access and events for investigation and resolution.

ISO: Information Security Officer.

Malicious Code: Malicious Code refers to code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target computer. They sometime masquerade as useful software or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include Trojan horses and computer viruses.

Media Access Control (MAC) address: A hardware address that uniquely identifies each node of a network.

Multi-User System: Multi-user system refers to computer systems that support two or more simultaneous users. All mainframes, servers and minicomputers are multi-user systems, but most personal computers, laptops and workstations are not.

Non-public Information: Any information that is protected from disclosure by law.

Owner of Information: An individual or organizational unit having responsibility for making protection and control decisions regarding use of information.

Penetration Testing: The portion of security testing in which evaluators attempt to exploit physical, network, system or application weaknesses to prove whether these weaknesses can be exploited by gaining extended, unauthorized or elevated privileged access to protected resources.

Personal Information: Personal information means any information concerning a natural person which, because of name, number, personal mark or other identifier, can be used to identify such natural person.

Physical Security: The protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Privacy: The right of individuals and organizations to control the collection, storage, and dissemination of information about themselves.

Private Information: Private Information means personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- social security number; or
- driver's license number or non-driver identification card number; or
- account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Privileged Account: The user-ID or account of an individual whose job responsibilities require special system authorization, such as a network administrator, security administrator, etc. Special authorizations are allocated to this account such as ACF2 Administrator, auditor, Special, UNIX root or Microsoft Administrator.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat.

Risk Management: The process of taking actions to assess risks and avoid or reduce risk to acceptable levels.

SE (Statewide Entity[ies]): Statewide Entities are individual organizations comprising the IT "enterprise'" as defined in the Statewide Information Technology Policies and Standards Glossary.

Security Administration: The actions and responsibility for administering the security mechanisms including identification and authentication establishment and authorization maintenance.

Security Management: The responsibility and actions required to manage the security environment including the security policies and mechanisms.

Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of information.

Sniffing: Monitoring network traffic.

Social Engineering: Manipulation of people to obtain security critical assets that allow security perils to take place.

Spamming: Blindly posting something to a large number of groups.

Spoofing: Representing yourself as someone else.

System(s): An interconnected set of information resources under the same direct management control that shares common functionality. A system may include hardware, software, information, data, applications or communications infrastructure.

Technical Security Review: A technical security review would consist of reviewing the controls built into a system or application to ensure they still perform as designed and are in compliance with documented security policies and procedures. It would also include reviewing security patches to ensure they have been installed and are operational, reviewing security rules such as access control lists for currency, testing of firewall rules, etc. This type of testing includes intrusion and/or penetration testing of controls.

Third Party: Any non-SE employees such as a contractor, vendor, consultant, intern, another SE, etc.

Threat: A force, organization or person, which seeks to gain access to, or compromise, information. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in risk assessment.

Trojan Horse: Illegal code hidden in a legitimate program that when executed performs some unauthorized activity or function.

Unauthorized Access Or Privileges: Access to network or computer resources without permission.

User: Any Statewide Entity(ies), federal government entity(ies), political subdivision(s), their employees or third party contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a System for a legitimate government purpose.

User of Information: An individual having specific limited authority from the Owner of Information to view, change, add to, disseminate or delete such information.

Virus: A program that replicates itself on computer systems by incorporating itself into other programs that are shared among computer systems. Once in the new host, a virus may damage data in the host's memory, display unwanted messages, crash the host or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).

Vulnerability: A weakness of a system or facility holding information which can be exploited to gain access or violate system integrity. Vulnerability can be assessed in terms of the means by which the attack would be successful.

Vulnerability Scanning: The portion of security testing in which evaluators attempt to identify physical, network, system or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.

Worm: A program similar to a virus that can consume large quantities of network bandwidth and spread from one network to another.

V. Roles and Responsibilities

Statewide Entity (SE): Each SE shall establish a framework to initiate and control the implementation of information technology security within the SE no later than the specific timelines delineated in Section V. Policy Requirements of this document. An Information Security Officer (ISO) shall be appointed. A process shall be established to determine information sensitivity, based on best practices, state directives, legal and regulatory requirements to determine the appropriate levels of protection for that information. The department head of each SE shall ensure that an organization structure is in place for:

- the implementation of information technology security policies and standards;
- assigning information technology security responsibilities;
- the implementation of a security awareness program;
- monitoring significant changes in the exposure of information assets to major threats, legal or regulatory requirements;
- responding to security incidents;
- the approval of major initiatives to enhance information technology security;
- the development of a process to measure compliance with this policy;
- the approval of new applications and services.

Department Heads: Department heads have overall responsibility for ensuring an adequate level of security for all data and implementation of this policy within the department.

SE Designated Staff: SE designated staff shall be responsible for the implementation of this and other information technology security policies and the compliance of SE employees to this policy. The designated staff shall educate SE employees with regard to information technology security issues. Staff shall explain the issues, why the policies have been established, and what role(s) individuals have in safeguarding information. Consequences of non-compliance shall also be explained.

Information Owners: An individual or a group of individuals designated by the SE shall serve as or represent information owners for the data and tools they use. Information owners are responsible for determining who shall have access to protected resources within their jurisdiction, and what those access privileges shall be (read, update, etc.). These access privileges shall be in accordance with the user’s job responsibilities. Information owners also communicate to the SE Information Security Officer (ISO) the legal requirements for access and disclosure of their data. Information owners shall be identified for all SE information assets and assigned responsibility for the maintenance of appropriate security measures such as assigning and maintaining asset protection and controls, managing user access to their resources, etc. Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the asset.

SE Information Security Officer (ISO): The SE Information Security Officer may be the same individual required by 2-15-114(2) MCA.

The SE Information Security Officer has overall responsibility for ensuring the implementation, enhancement, monitoring and enforcement of the information technology security policies and standards. The SE Information Security Officer is responsible for providing direction and leadership to his or her SE through the recommendation of security policies, standards, processes and education and awareness programs to ensure that appropriate safeguards are implemented, and to facilitate compliance with those policies, standards and processes.

The SE Information Security Officer is responsible for investigating real or suspected information technology security violations. In this role, the SE Information Security Officer shall follow SE procedures for referring the investigation to other investigatory entities, including law enforcement. The SE Information Security Officer shall coordinate and oversee security program activities and reporting processes in support of this policy and other security initiatives.

The SE Information Security Officer is responsible for performing, at a minimum, the following tasks:

- coordinate the development and implementation of information technology security policies, standards, procedures, and other control processes that meet the business needs of the SE;
- provide consultation for the various SE computing platforms;
- work closely with security administration or those serving in that function to ensure security measures are implemented to meet policy requirements;
- evaluate new security threats and counter measures that could affect the SE and make appropriate recommendations to the SE's CIO and other management to mitigate the risks;
- review and approve all external network connections to the SE's network;
- provide consultation to the SE management with regard to all information technology security;
- investigate and report to appropriate internal management and enterprise IT security office according to the enterprise IT security

office incident reporting standard; (This requirement will be in effect when the standard is approved.)

- ensure that appropriate follow-up to security violations is conducted;
- ensure appropriate information technology security awareness and education to all SE employees, and where appropriate, to third party individuals;
- be aware of laws and regulations that could affect the security controls and protection requirements of the SE's information;
- complete a minimum of twenty two and half (22.5) hours of Continuing Professional Education (CPE) credits annually in order to maintain an adequate level of current knowledge and proficiency in information technology security. The CPEs shall be directly related to information systems security.

Security Administrators: When such an individual or individuals exist, the individual or individuals shall work closely with the SE Information Security Officer and support staff. Security Administrators are the staff normally responsible for administering security tools, reviewing security practices, identifying and analyzing security threats and solutions, and responding to security violations. This individual or individuals has administrative responsibility over all user-IDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements. Where a formal security administration function does not exist, the organization or staff responsible for the security administration functions described above shall comply with this policy.

Senior SE Information Technology (IT) Manager: The senior SE IT manager has responsibility for the data processing infrastructure and computing network which support the information owners. It is the responsibility of senior SE IT manager to facilitate overall SE compliance with this policy and provide the resources needed to enhance and maintain a level of IT security control consistent with their SE's Information Technology Security Policy.

Senior SE IT managers have the following responsibilities in relation to the security of information:

- ensuring processes, policies and requirements are identified and implemented relative to security requirements defined by the SE's business;
- ensuring the proper controls of information are implemented for which the SE's business have assigned ownership responsibility, based on the SE's levels of protection;
- ensuring the participation of the SE Information Security Officer and technical staff in identifying and selecting appropriate and cost-

effective security controls and procedures, and in protecting information assets;

- ensuring that appropriate security requirements for user access to automated information are defined for files, databases, and physical devices assigned to their areas of responsibility;
- ensuring that critical data and recovery plans are backed up and kept at a secured off-site storage facility and that recovery of backed-up media shall work if and when needed.

SE Employees: It is the responsibility of all employees to protect SE information and resources, including passwords, and to report suspected security incidents to the appropriate manager and the SE Information Security Officer.

Non-SE Employees: Individuals who work under agreements with the SE such as Contractors, Consultants, Vendors, volunteers and other persons in similar positions, to the extent of their present or past access to SE information, are also covered by this Information Technology Security Policy. Just like SE employees, each non-SE employee has the individual responsibility to protect SE information and resources, including passwords, and to report suspected security incidents to the appropriate manager and the SE Information Security Officer.

The Chief Information Officer: The State of Montana Chief Information Officer is the owner of this policy and provides, staffs and oversees the enterprise IT security office, and other resources and functions required to oversee implementation and compliance to this policy.

The Enterprise IT Security Office: The enterprise IT security office performs as the security consultant to SE ISOs and SEs. The office may also perform periodic reviews of SE security programs for compliance with this and other security policies and standards. The office establishes and monitors effectiveness of IT security policies, standards, procedures and controls statewide.

VI. Policy Requirements

A. Information Related Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2010.

Information and information assets accessed, stored, used or supported *by statewide IT facilities or assets* shall be subject to the following requirements:

Information, regardless of the form or format, which is created, acquired or used in support of SE's business activities, shall only be used for SE business. SE information is an asset and shall be protected from its creation, through its useful life, and to its authorized disposal. It shall be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. Information shall be protected based on its importance to business activities, risks, and security best practices.

A process shall be established to determine information sensitivity, based on best practices, state directives, legal and regulatory requirements to determine the appropriate levels of protection for that information.

SE-designated staff is responsible for ensuring that appropriate physical, logical and procedural controls are in place on these assets to preserve the security properties of confidentiality, integrity, availability and privacy of SE information.

1. Individual Accountability Requirements

Individual accountability shall be instituted and enforced by SEs.

- Access to SE computer, computer systems and networks where the information owner has identified the business need for limited user access or information integrity and accountability, shall be provided through the use of individually assigned unique computer identifiers, known as user-IDs, or other technologies including biometrics, token cards, etc.
- Individuals who use SE computers shall only access information assets to which they are authorized.
- Associated with each user-ID is an authentication token, such as a password, which shall be used to authenticate the person accessing the data, system or network. Passwords, tokens or similar technology shall be treated as confidential information, and shall not be disclosed. Where technically feasible, transmission of such authentication information shall use secure mechanisms.
- Each individual is responsible to reasonably protect against unauthorized activities performed under their user-ID.

- For the user's protection, and for the protection of SE resources, user-IDs and passwords (or other tokens or mechanisms used to uniquely identify an individual) shall not be shared. (Refer to Access Control Requirements, Operating System Access Control.)

2. Confidentiality / Integrity / Availability Requirements

All SE information shall be protected from unauthorized access to help ensure the information's confidentiality and maintain its integrity. The information owner shall define the required level of protection and secure information within their jurisdiction based on the information's value, sensitivity to disclosure, consequences of loss or compromise, and ease of recovery.

Appropriate processes shall be defined in the SE recovery plan and implemented to ensure the reasonable and timely recovery of all SE information, applications, systems and security regardless of computing platform, should that information become corrupted, destroyed, or unavailable for a defined period. (Refer to Operational Management Requirements, Information Backup.)

B. Organizational IT Security Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2010.

Each SE shall establish an IT security function led by an ISO. The SE ISO shall report to a high-level individual in the organization or directly to the Chief Information Officer (CIO), but not an IT manager or director, to balance security with technological and programmatic issues. If the CIO is an IT manager, administrator or director, the ISO shall report to another equivalent-level position. The mission of the IT Security Function is to:

- develop, deploy and maintain an information technology security architecture that shall provide security policies, mechanisms, processes, standards and procedures that meet current and future business needs of the SE. Such architectures shall not conflict with enterprise IT architectures;
- provide information technology security advice to the SE regarding security threats that could affect the SE computing and business operations, and make recommendations to mitigate the risks associated with these threats;
- assist management in the implementation of security measures that meet the business needs of the individual SE;
- develop and implement security training and awareness programs that educate SE employees, contractors and vendors with regard to the SE's information technology security requirements;

- investigate and report to management breaches of security controls, and implement additional compensating controls when necessary to help ensure security safeguards are maintained;
- participate in the development, implementation and maintenance of disaster recovery processes and techniques to ensure the continuity of the SE's business and the security controls, in the event of an extended period of computing resource unavailability;
- although IT security roles & responsibilities may be outsourced to third parties, it is the responsibility of each SE to maintain control and accountability of the security of the information that it owns.
- Define and maintain the SE's security plan, and provide it to the statewide IT planning function.

C. Information Protection and Control Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2010.

Information is an asset and shall be properly managed from its creation, through authorized use, to proper disposal. As with other assets, not all information has the same use or value, and therefore information requires different levels of protection. All information shall be protected and managed based on its confidentiality, integrity and availability characteristics.

All information shall have an information owner established within the SE's lines of business who shall be responsible for assigning the initial information levels of protection, and make all decisions regarding controls, access privileges of users, and daily decisions regarding information management. Periodic high-level business impact analyses shall be performed on the information to determine its relative value, risk of compromise, etc. Based on the results of the assessment, information shall be categorized into one of the SE's information levels of protection.

Each level of protection shall have a set or range of controls, designed to provide appropriate protection of the information and its associated application software commensurate with the value of the information. If this information is stored by a third-party, the third-party shall contractually abide by these rules.

D. Personnel Security Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2009.

The intent of this requirement is to reduce the risk of human error and misuse of SE information and facilities to an acceptable level.

1. Including Security in Job Responsibilities

Security roles and responsibilities shall be documented. These roles and responsibilities shall include general responsibilities for all SE employees, as well as specific responsibilities for protecting specific information and performing tasks related to security procedures or processes. Additional security roles and responsibilities for those individuals responsible for information technology security are defined in this document, Organizational Security Requirements.

2. User Training

All individuals with access to SE information shall receive security awareness training to ensure they are knowledgeable of security procedures, their role and responsibilities regarding the protection of SE information, and the proper use of information processing facilities to minimize security risks.

An information technology security awareness program shall be developed, implemented and maintained that addresses the security education needs of all SE employees. A SE security awareness program shall be developed by the SE's Information Security Officer to supplement the SE's new employee orientation program, and shall be reinforced at least annually.

3. Security Incidents or Malfunctions Management Process

Formal incident or malfunction reporting and response procedures shall be established, that define the actions to be taken when an incident occurs. The following shall be included:

- the symptoms of the problem and any messages displayed shall be documented;
- where appropriate, the computer shall be isolated, if possible, and use of it stopped until the problem has been identified and resolved;
- the incident shall be reported immediately to the appropriate SE manager and the SE ISO.

Feedback mechanisms shall be implemented to ensure that individuals reporting incidents are notified of the results after the incident has been resolved and closed.

An incident management process shall be established to track the types and volumes of security incidents and malfunctions. This information shall be used by the SE to identify recurring or high impact incidents and to record lessons learned. This may indicate the need for additional controls to limit the frequency, damage and cost of future incidents, or to be taken into account in the policy review process.

State employees and contractors shall not attempt to prove a suspected weakness unless authorized by the SE ISO to do so. Testing weaknesses could have unintended consequences.

All users of SE systems shall be made aware of the procedure for reporting security incidents, threats or malfunctions that may have an impact on the security of SE information. All SE staff and contractors are required to report any observed or suspected incidents to the appropriate manager and the SE ISO as quickly as possible.

Approaches to incident management shall be documented and procedures shall be clearly identified to ensure responsibilities are defined, resulting in a prompt and organized response to security incidents.

Incident response procedures shall be clearly identified to promote effective response to security incidents. Include procedures for information system failure, denial of service, disclosure of confidential information and compromised systems of software. Once an incident has been identified, the following procedures shall be followed:

- report the action to the enterprise IT security office according to the enterprise IT security office incident reporting standard (This requirement will be in effect when the standard is approved.);
- identify the underlying cause of the incident;
- identify procedures the SE shall employ to resolve the problem
- identify procedures the SE shall employ to prevent the same or similar incident from occurring;
- track the response procedure from initial report through follow-up for review and audit purposes; and,
- provide adequate follow-up to ensure that individuals involved or affected by the incident understand what took place and how the incident was resolved.

E. Physical and Environmental Security Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2010.

Critical or sensitive SE business information processing and storage facilities shall be contained in secure areas protected by a defined security perimeter, with appropriate security barriers and some form of access controls. Physical protection measures shall be implemented to protect the facility from unauthorized access, damage and interference.

The SE may include physical security, such as controlling access to the building, etc. The SE shall perform periodic threat and risk analysis to determine where additional physical security measures are necessary, and implement these measures to mitigate the risks.

1. Physical Security Perimeter

The purpose of the security perimeter is to prevent unauthorized access or theft of information or information assets. Breaching of a physical security perimeter can cause a loss of or damage to SE information. Effective physical security perimeters can be achieved by creating a number of physical barriers around the assets being protected. Each barrier establishes a security perimeter that would require a method of access control to gain entry. This perimeter could be in the form of an entry point with card key access, a staffed reception area, a locked cabinet or office or other physical barrier.

The SE shall perform a threat and risk assessment to determine the extent of the perimeter, and types of controls necessary to mitigate the risk. Based on the threat and risk assessment, a physical security perimeter shall be established in SE environments where information or information assets are stored or operational, SE data centers, wiring closets for network and telephonic connections, printers where confidential or sensitive information may be printed, and any other location where information may be in use or stored.

2. Equipment Security

Computer equipment shall be physically protected from security threats and environmental hazards. Protection of computer equipment is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. Special controls may also be necessary to protect supporting facilities such as electrical supply and cabling infrastructure. This protection shall include but is not limited to data centers, wiring closets, server rooms, and storage facilities where computers and computer peripherals are stored.

3. Secure Disposal or Re-use of Storage Media and Equipment

There is risk of disclosure of sensitive information through careless disposal or re-use of equipment. Formal processes shall be established to minimize this risk. Storage devices such as hard disk drives and other media (e.g. tape, diskette, CDs, DVDs, cell phones, digital copiers or other devices that store information) or paper containing sensitive information shall be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive SE information.

4. Clear Screen

To prevent unauthorized access to information, automated techniques and controls shall be implemented to require authentication or re-authentication after a predetermined period of inactivity for desktops, laptops, PDA’s and any other computer systems where authentication is required. These controls may include such techniques as password protected screen savers, automated logoff processes, or re-authentication after a set time out period.

F. Communications and Network Management Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2011.

All SE networks shall implement appropriate security controls to ensure the integrity of the data flowing across these networks. If there is a business need, additional measures to ensure the confidentiality of the data shall also be implemented.

The SE ISO shall ensure that measures are in place to mitigate any new security risks created by connecting the SE networks to a third party network.

Where a SE has outsourced a server or application to a third party service (such as web applications), the SE ISO shall perform or have performed periodic security reviews of the outsourced environment to ensure the security and availability of the SE’s information and application.

All connections to the SE networks shall be authorized by the appropriate Network Manager, and reviewed by the SE ISO. Additions or changes to network configurations shall also be reviewed and approved through the SE Change Management process.

1. Sharing Information Outside Statewide Entity

To facilitate the secure sharing of information, appropriate security measures shall be in place commensurate with the sensitivity and confidentiality of the information being shared. In most cases, the security confidentiality requirements of the data being shared shall determine the level of security required when sharing data.

For information to be released outside an SE or shared between SEs, a process shall be established that, at a minimum:

- evaluates and documents the sensitivity of the information to be released or shared;
- identifies the responsibilities of each party for protecting the information;
- defines the minimum controls required to transmit and use the information;
- records the measures that each party has in place to protect the information;
- defines a method for compliance measurement;

- provides a signoff procedure for each party to accept responsibilities;
- establishes a schedule and procedure for reviewing the controls.

2. Network Management

All SEs shall implement a range of network controls to maintain security in its trusted, internal network, and ensure the protection of connected services and networks. These controls help prevent unauthorized access and use of the SE private network. The following controls, at a minimum shall be implemented:

- Operational responsibility for networks shall be separate from computer operations when possible;
- Responsibilities and procedures for remote use shall be established (refer to Access Control Requirements section of this document);
- When necessary, special controls shall be implemented to safeguard data integrity and confidentiality of data passing over public networks (Internet).

3. Vulnerability Scanning

All SE owned hosts that are or shall be accessible from outside the SE network shall be scanned for vulnerabilities and weaknesses before being installed on the network, and after software, operating system or configuration changes are made. For both internal and external systems, scans shall be performed at least annually to ensure that no major vulnerabilities have been introduced into the environment. The frequency of additional scans shall be determined by the SE ISO and the information owner(s), depending on the criticality and sensitivity of the information on the system.

Network vulnerability scanning shall be conducted after new network software or major configuration changes have been made on systems that are essential to supporting a process that is critical to a SE business, and annually on all other systems. The output of the scans shall be reviewed in a timely manner by the SE ISO, and any vulnerability detected shall be evaluated for risk and mitigated. The tools used to scan for vulnerabilities shall be updated periodically to ensure that recently discovered vulnerabilities are included in any scans.

Where a SE has outsourced a server, application or network services to another SE, responsibility for vulnerability scanning shall be coordinated by both SEs.

Anyone authorized to perform vulnerability scanning shall have a process defined, tested and followed at all times to minimize the possibility of disruption. Reports of exposures to vulnerabilities shall be forwarded to the SE ISO and other defined staff.

Any vulnerability scanning other than that performed by enterprise IT security office shall be conducted by individuals who are authorized by the SE ISO.

4. Penetration & Intrusion Testing

All SE computing systems that provide information through a public network, either directly or through another service that provides information externally (such as the World Wide Web), shall be subjected to SE penetration analysis and intrusion testing. Such analysis and testing shall be used to determine if:

- an individual can make an unauthorized change to an application;
- a user may access the application and cause it to perform unauthorized tasks;
- an unauthorized individual may access, destroy or change any data; or
- an unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).

The output of the penetration testing and intrusion testing shall be reviewed in a timely manner by the SE ISO, and any vulnerability detected shall be evaluated for risk and mitigated as appropriate.

The tools used to perform the penetration testing shall be updated to ensure that recently discovered vulnerabilities are included in any testing.

Where a SE has outsourced a server, application or network services to another SE, penetration testing shall be coordinated by both SEs.

Only individuals authorized by the SE shall perform penetration testing. The SE ISO shall approve and the enterprise IT security office shall be notified 24 hours prior to each penetration test. Any other attempts to perform such penetration testing shall be deemed an unauthorized access attempt.

5. Internet and Electronic Mail Acceptable Use

When SE employees connect to the Internet using any SE Internet address designation or send electronic mail using the SE designation, it shall be for purposes authorized by SE management. The following is not an all-inclusive list, and provides only examples of behavior that could result in security breaches. Specifically, the Internet and electronic mail shall not be used:

- to represent yourself as someone else (i.e., “spoofing”);
- for spamming;
- for unauthorized attempts to break into any computing system whether SE’s or another organization’s (i.e., cracking or hacking);
- for theft or unauthorized copying of electronic files;
- for posting sensitive SE information without authorization from SE;
- for any activity which create a denial of service, such as “chain letters”;

- for “sniffing” (i.e., monitoring network traffic), except for those authorized to do so as part of their job responsibilities.

6. External Connections

(Also see Access Control Requirements, User Authentication for External Connections, Remote Access Control Requirements)

Because the Internet is inherently insecure, access to the Internet is prohibited from any device that is connected, wired or wireless to any part of a SE network unless specifically authorized by SE ISO. This includes accounts with third party Internet service providers. Users shall not use the SE’s Internet accounts to establish connections to these third party services, unless authorized to do so by SE management and the security of the connection is reviewed and approved by the SE ISO.

All connections from the SE network to external networks shall be approved in writing by the SE ISO. Connections shall be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures, or appropriate security measures have been implemented by the SE to protect SE network resources. A risk analysis shall be performed to ensure that the connection to the external network shall not compromise the SE’s private network. Additional controls, such as the establishment of firewalls and a DMZ (demilitarized zone) may be implemented between the third party and the SE. These connections shall be periodically reviewed by the SE to ensure:

- the business case for the connection is still valid and the connection is still required;
- the security controls in place (filters, rules, access control lists, etc.) are current and functioning correctly.

This policy requires that connection to the SE network be done in a secure manner to preserve the integrity of the SE network, data transmitted over that network, and the availability of the network. The security requirements for each connection shall be assessed individually, and be driven by the business needs of the parties involved. Only SE authorized, qualified staff or qualified third party shall be permitted to use sniffers or similar technology on the network to monitor operational data and security events

The SE ISO or designee shall regularly review audit trails and system logs of external network connections for abuses and anomalies.

Third party network and/or workstation connection to a SE network shall have an internal SE sponsor develop a business case for the network connection. A SE non-disclosure agreement shall be signed by a duly appointed representative from the third party organization who is legally authorized to sign such an agreement. In addition to the agreement, the third party’s equipment shall also conform to the state's security policies and standards, and be approved for connection by the SE ISO.

Any connection between SE firewalls over external networks that involves sensitive information shall use encryption to ensure the confidentiality and integrity of the data passing over the external network.

7. Security of Electronic Mail

Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. Users of the SE email system are a visible representative of the state and shall use the systems in a legal, professional and responsible manner. Unless prior management approval has been obtained, SE users shall not connect to commercial email systems from any SE system or workstation (i.e., AOL, Yahoo, etc.). Users of SE email systems shall comply with this policy and be knowledgeable of their responsibilities as defined in Communications and Network Management Requirements, Internet and Electronic Mail Acceptable Use Requirements.

8. Portable Devices

All portable computing resources and information media shall be secured to prevent compromise of confidentiality or integrity. No computer device may store or transmit non-public information without suitable protective measures that are approved by the SE ISO.

When using mobile computing facilities such as notebooks, palmtops, laptops and mobile phones, special care shall be taken to ensure that information is not compromised. Approval is contingent on satisfaction of the requirements for physical protection, access controls, cryptographic techniques, back-ups, virus protection and the rules associated with connecting mobile facilities to networks and guidance on the use of these facilities in public places.

- Care shall be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the SE's premises. Protection shall be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques.
- It is important that when such facilities are used in public places care shall be taken to avoid the risk of unauthorized persons viewing information on-screen.
- Procedures against malicious software shall be developed and implemented and be kept up to date. Equipment shall be available to enable the quick and easy back up of information. These back-ups shall be given adequate protection against theft or loss of information.

- Equipment carrying important, sensitive and/or critical business information shall not be left unattended and, where possible, shall be physically locked away, or special locks shall be used to secure the equipment.
- Training shall be provided to staff using mobile computing resources to raise their awareness on the additional risks resulting from this way of working and the controls that shall be implemented.
- Employees in the possession of portable, laptop, notebook, palmtop, and other transportable computers shall not check these computers in airline luggage systems. These computers shall remain in the possession of the traveler as hand luggage unless other arrangements are required by Federal or State authorities.

9. Telephones and Fax Equipment

The use of telephones outside the SE for business reasons is sometimes necessary, but it can create security exposures. Employees shall:

- take care that they are not overheard when discussing sensitive or confidential matters;
- avoid use of any wireless or cellular phones when discussing sensitive or confidential information;
- avoid leaving sensitive or confidential messages on voicemail systems;
- if sending sensitive or confidential documents via fax, verify the phone number of the destination fax. Contact the recipient to ensure protection of the fax, either by having it picked up quickly or by ensuring that the fax output is in a secure area;
- avoid using Internet fax services to send or receive sensitive or confidential information;
- not use third party fax services to send or receive sensitive or confidential information;
- not send sensitive or confidential documents via wireless fax devices;
- not send teleconference call-in numbers and passcodes to a pager, if sensitive or confidential information shall be discussed during the conference;
- when chairing a sensitive or confidential teleconference, confirm that all participants are authorized to participate, before starting any discussion.

10. Wireless Networks

Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However security risks, if not addressed correctly, could expose SE information systems to a loss of service or compromise of sensitive information.

Wireless is a shared medium. Everything that is transmitted over the radio waves can be intercepted if the interceptor is within the coverage area of the radio transmitters. This represents a potential security issue in the wireless Local Area Networks (LANs). The security exposure is more evident if the wireless LANs are deployed or used in public areas, such as airports, hotels or conference centers.

No wireless network or wireless access point shall be installed without a risk assessment being performed and the written approval of the SE ISO.

Suitable controls, such as Media Access Control (MAC) address restriction, authentication and encryption shall be implemented to ensure that a wireless network or access point can not be exploited to disrupt SE information services or to gain unauthorized access to SE information. When selecting wireless technologies, wireless network security features on the equipment shall be available and implemented from the beginning of the deployment using current best practices.

Access to systems that hold non-public information or the transmission of non-public or sensitive information via a wireless network is not permitted unless appropriate and adequate measures have been implemented and approved by the SE ISO. Such measures shall include authentication, authorization, access controls and logging (refer to Access Control Requirements, Monitoring System Access and Use Requirements).

11. Modem Usage

Connecting dial-up modems to computer systems which are also connected to SE’s local area network or to another internal communication network is prohibited unless the SE ISO approves the request, a risk assessment is performed and risks are appropriately mitigated.

12. Public Websites Content Approval Process

The World Wide Web provides an opportunity for SEs both to disseminate information and to provide interactive government services quickly and cost effectively. Because anything posted on a public web server is globally available and each web presence is a potential connection path to SE networks, care shall be exercised in the deployment of publicly accessible servers. There is also potential for an insecure server to be used or exploited to assist in an unauthorized or illegal activity, such as an attack on another web site.

The content of each public site shall be reviewed according to a process that shall be defined and approved by the SE. A process shall be established for reviewing and approving updates to publicly available content. These reviews shall include consideration of copyright issues (both the potential publication of copyright material and the appropriate protection of SE copyright materials), the type of information being made available (confidentiality, privacy and sensitivity of the information), the accuracy of the information and potential legal implications of providing the information.

Sensitive or confidential State information shall not be made available through a server that is available to a public network without appropriate safeguards approved by the SE ISO. The SE ISO shall implement safeguards to ensure user authentication, data confidentiality and integrity, access control, data protection and logging mechanisms.

The design of a hosting service shall be reviewed and approved in writing by the SE ISO to ensure that the security of the web server, protection of SE networks, performance of the site, integrity and availability requirements are adequately addressed.

The implementation of any web site or software subject to all requirements set forth in Systems Development and Maintenance Requirements. The service shall be reviewed and approved by the SE ISO to ensure that the collection and processing of information meets SE security and privacy requirements. The review shall ensure that the information is adequately protected in transit over public and SE networks, in storage and while being processed.

13. Electronic Signatures

SEs shall comply with any State law(s) and associated rules and regulations.

14. Public Key Infrastructure

The establishment of Public Key Infrastructure (PKI) based security architecture is a significant undertaking that requires the establishment of the required business processes to support the PKI and the implementation of technology to support the resulting business processes. In order for the SE to operate with a PKI based Security Architecture, the following requirements shall be satisfied.

- An appropriate trust model shall be defined to include all of the stakeholders. The resulting trust domain or multiple trust domains shall be supported by the appropriate certificate policies and certification practice statements. These apply to the stakeholders and users of SE systems and data.
- Where PKI is used for digital signatures or encryption, it shall operate under and comply with the State certificate standards for digital signatures and encryption and any associated rules and regulations. (This requirement will be in effect when the standards are approved.)

G. Operational Management Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2010.

All SE information processing facilities shall have documented operating instructions, management processes and formal incident management procedures related to information technology security matters, that define roles and responsibilities of affected individuals who operate or use SE information processing facilities.

Computing hardware, software or system configurations provided by SE shall not be altered or added to in any way unless exempted by documented written policy, procedures or specific written approval of SE management.

Where a SE provides a server, application or network services to another SE, operational and management responsibilities shall be coordinated by both SEs.

1. Development Requirements

(a) Segregation of Security Duties

To reduce the risk of accidental or deliberate system misuse, separation of duties or areas of responsibility shall be implemented where practical.

Whenever separation of duties is difficult to achieve, other compensatory controls such as monitoring of activities, audit trails and management supervision shall be implemented. At a minimum the audit of security shall remain independent and segregated from the security function.

(b) Separation of Development, Test and Production Environments

Separation of the development, test and production environments is required, either logically or physically. Processes shall be documented and implemented to govern the transfer of software from the development environment to the production platform. The following controls shall be implemented:

- development software and tools shall be maintained on computer systems isolated from the production environment. Contain development software on physically separate machines or separate them by access controlled domains or directories;
- access to compilers, editors and other system utilities shall be removed from production systems when not required;
- logon procedures and environmental identification shall be sufficiently unique for production testing and development;

- Controls shall be in place to issue short-term access to development staff to correct problems with production systems allowing only necessary access.

Development and testing can cause serious problems to the production environment if separation of these environments does not exist. The degree of separation between the production and test environments shall be considered by each SE to ensure adequate protection of the production environment.

Separation shall also be implemented between development and test functions. Each SE shall use a stable quality assurance environment where user acceptance testing can be conducted and changes cannot be made to the programs being tested.

(c) System Planning and Acceptance

Because system and data availability is a security concern, advance planning and preparation shall be performed to ensure the availability of adequate capacity and resources. The security requirements of new systems shall be established, documented and tested prior to their acceptance and use.

Storage and memory capacity demands shall be monitored and future capacity requirements projected to ensure adequate processing and storage capability is available when needed. This information shall be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.

Acceptance criteria shall be developed and documented for new information systems, upgrades and new versions of existing systems. Acceptance testing shall be performed to ensure security requirements are met prior to the system being migrated to the production environment. SE managers shall ensure that the security requirements and criteria for acceptance are clearly defined, agreed, documented and tested.

(d) Protection against Malicious Code

Software and associated controls shall be implemented across SE systems to prevent and detect the introduction of malicious code. The introduction of malicious code such as a computer virus, network worm program and Trojan horse can cause serious damage to networks, workstations and business data. Users shall be made aware of the dangers of unauthorized or malicious code. SE shall implement controls to detect and prevent a computer virus from being introduced to the SE environment. The types of controls and frequency of updating signature files, is dependent on the value and sensitivity of the information that could be potentially at risk. For most SE workstations, virus signature files shall be updated weekly. On host systems or servers, the files shall be updated daily or when the virus software vendor’s signature files are updated and published.

(e) Software Maintenance

All system software shall be maintained at a vendor-supported level to ensure software accuracy and integrity, unless SE ISO approves otherwise in writing.

Maintenance of SE-developed software shall be logged to ensure changes are authorized, tested and accepted by SE management.

All known security patches shall be reviewed, evaluated and appropriately applied in a timely manner to reduce the risk of security incidents that could affect the confidentiality, integrity and availability of business data or software integrity.

(f) Information Back-up

The scope of this section is limited to the IT infrastructure, and the data and applications of the local SE environment. A threat and risk assessment shall be performed by the SE to determine the criticality of business systems, and the time frame required for recovery. To ensure interruptions to normal SE business operations are minimized, and critical SE business applications and processes are protected from the effects of major failures, each SE business unit, including SE Security Management, in cooperation with the SE CIO, shall develop plans that can meet the IT backup and recovery requirements of the SE. Back-ups of critical SE data and software shall be performed regularly.

(g) Assessment

An assessment of the criticality of the services provided and the sensitivity of the information held on all hosts and servers (including all installed software and operating system versions, firewalls, switches, routers and other communication equipment operating systems) shall be maintained.

(h) System Security Checking

Systems and services that process or store sensitive or confidential information or provide support for critical processes shall undergo technical security reviews to ensure compliance with implementation standards and for vulnerabilities to subsequently discovered threats. Reviews of systems and services that are essential to supporting a critical SE function shall be conducted at least once every year. Reviews of a representative sample of all other systems and services shall be conducted at least once every twenty-four months.

Any deviations from expected or required results that are detected by the technical security review process shall be reported to the SE ISO and corrected immediately. In addition, the SE application owner shall be advised of the deviations and shall initiate investigation of the deviations (including the review of system activity log records if necessary).

H. Access Control Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2011.

To preserve the properties of integrity, confidentiality and availability, the SE’s information assets shall be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery of these assets.

Information owners are responsible for determining who shall have access to protected resources within their jurisdiction, and what those access privileges shall be (read, update, etc.). These access privileges shall be granted in accordance with the user’s job responsibilities.

1. User Registration and Management

A user management process shall be established and documented by the SE to outline and identify all functions of user management, to include the generation, distribution, modification and deletion of user accounts for access to resources. The purpose of this process is to ensure that only authorized individuals have access to SE applications and information and that these users only have access to the resources required for authorized purposes.

The user management process shall include the following sub-processes as appropriate:

- enrolling new users;
- removing user-IDs;
- granting “privileged accounts” to a user;
- removing “privileged accounts” from a user;
- periodic reviewing “privileged accounts” of users;
- periodic reviewing of users enrolled to any system; and
- assigning a new authentication token (e.g. password reset processing).

The appropriate information owner or other authorized officer shall make requests for the registration and granting of access rights for State employees.

For applications that interact with individuals that are not employed by an SE, the information owner is responsible for ensuring an appropriate user management process is implemented. Standards for the registration of such external users shall be defined, to include the credentials that shall be provided to prove the identity of the user requesting registration, validation of the request and the scope of access that may be provided.

2. Logon Banner

Logon banners shall be implemented on all systems where that feature exists to inform all users that the system is for SE business or other approved use consistent with SE policy, and that user activities may be monitored and the user should have no expectation of privacy. Logon banners are usually presented during the authentication process.

3. Privileged Accounts Management

The issuance and use of privileged accounts shall be restricted and controlled. Inappropriate use of system account privileges is often found to be a major contributing factor to the failure of systems that have been breached. Processes shall be developed to ensure that uses of privileged accounts are monitored, and any suspected misuse of these accounts is promptly investigated. Passwords of multi-user system privileged accounts shall be changed more often than normal user accounts.

4. User Password Management

Passwords are a common means of authenticating a user's identity to access an information system or service. Password standards shall be developed and implemented to ensure all authorized individuals accessing SE resources follow proven password management practices. These password rules shall be mandated by automated system controls whenever possible. These password best practices include but are not limited to:

- passwords shall not be stored in clear text;
- use passwords that are not easily guessed or subject to disclosure through a dictionary attack;
- keep passwords confidential – do not share individual;
- change passwords at regular intervals;
- change temporary passwords at the first logon;
- when technology permits, passwords shall contain a mix of alphabetic, numeric, special, and upper/lower case characters; and
- do not include passwords in any automated logon process, e.g., stored in a macro or function key, web browser or in application code

To ensure good password management, password standards shall be implemented on all SE platforms where technically feasible.

5. Network Access Control

Access to a SE's trusted internal network shall require all authorized users/device to authenticate themselves through use of an individually assigned user-ID and an authentication mechanism; e.g., password, token, smart card. Network controls shall be developed and implemented that ensure that an authorized user can access only those network resources and services necessary to perform their assigned job responsibilities. Network controls shall be developed and implemented that ensure that a device is in compliance with policy and can access only those network resources and services for which they are authorized.

6. User Authentication for External Connections (Remote Access Control)

(Also see Communication and Network Management Requirements, External Connections)

To maintain information technology security, SE requires that individual accountability be maintained at all times, including during remote access. For the purposes of this policy, “remote access” is defined as any access coming into the SE’s network from off the SE’s private, trusted network. This includes, but is not limited to:

- dialing in from another location over public lines by an employee or other authorized individual for the purpose of telecommuting or working from home;
- connecting a third party network via dial or other temporary access technology to the SE network;

Connection to SE’s networks shall be done in a secure manner to preserve the integrity of the network, data transmitted over that network, and the availability of the network. Security mechanisms shall be in place to control access to SE systems and networks remotely from fixed or mobile locations.

Advance approval for any such connection shall be obtained from the SE management and the SE ISO. An assessment shall be performed and documented to determine the scope and method of access, the risks involved and the contractual, process and technical controls required for such connection to take place.

Because of the level of risk inherent with remote access, use of a stronger password or another comparable method is required prior to connecting to any SE network. All sessions are subject to periodic and random monitoring.

When accessing a SE network remotely, identification and authentication of the entity requesting access shall be performed in such a manner as to not disclose the password or other authentication information that could be intercepted and used by a third party.

Use of a common access point is required. This means that all remote connections to a computer shall be made through managed central points-of-entry. Using this type of entry system to access a SE computer provides many benefits, including simplified and cost effective security, maintenance, and support.

For a vendor to access SE computers or software, individual accountability is also required. For those systems (hardware or software) for which there is a built-in user-ID for periodic maintenance, the account shall be disabled until the user-ID is needed. The activity performed while this vendor user-ID is in use shall be logged. Since these accounts are not regularly used, the vendor user-ID shall be disabled, the password changed or other controls implemented to prevent or monitor unauthorized use of these privileged accounts during periods of inactivity.

In the special case where servers, storage devices or other computer equipment has the capability to automatically connect to a vendor to report problems or suspected problems, the SE ISO shall review any such connection and process to ensure that connectivity does not compromise the SE or other third party connections.

Working from a remote location shall be authorized by SE management and appropriate arrangements made for this activity through written policy and procedure, to ensure the work environment at the remote location provides adequate security for SE data and computing resources. Appropriate protection mechanisms commensurate with risk and exposure shall be in place to protect against theft of SE equipment, unauthorized disclosure of SE information, misuse of SE equipment or unauthorized access to the SE internal network or other facilities by anyone including family and friends. To ensure the proper security controls are in place and all SE security standards are followed, the following shall be evaluated. If/when implemented, they shall be monitored and audited:

- the physical security of the remote location including using a laptop at any location other than an employee's work station; and,
- the accessing mechanism given the sensitivity of SE's internal system the sensitivity of and method of transmitting information.
- appropriate business continuity procedures including backing up critical information.

The following controls shall be evaluated and appropriately implemented. If/when implemented, they shall be monitored and audited:

- a definition of the levels of protection of the information and the systems and services that the remote user is authorized to access;
- documented procedures and necessary tools allowing for secure remote access such as authentication tokens and/or passwords, including procedures for revocation of authorization and return of equipment;

- hardware and software support and maintenance procedures including anti-virus software and maintenance of current signature files;
- implementation of suitable network boundary controls to prevent unauthorized information exchange between SE networks connected to remote computers and externally connected networks, such as the Internet. Such measures include firewalls and intrusion detection techniques at the remote location;
- encryption of sensitive information in transit and on the local computer workstation;
- physical security of the equipment used for remote access (e.g. such as cable locking device, or locking computer cabinet/secure storage area);

7. Segregation/Compartmentalization of Networks

When the SE network is connected to another network, or becomes a segment on a larger network, controls shall be in place to prevent users from other connected networks access to sensitive areas of the SE's private network. Firewalls, routers, or other technologies shall be implemented to control access to secured resources on the trusted SE network.

8. Operating System Access Control

Access to operating system code, services and commands shall be restricted to only those individuals necessary in the normal performance of their job responsibilities. All individuals (systems programmers, database administrators, network and security administrators, etc.) shall have a unique privileged account (user-ID) for their personal and sole use so that activities can be traced to the responsible person. User-IDs shall not give any indication of the user's privilege level, e.g., supervisor, manager, administrator. These individuals shall also have a second user-ID when performing normal business transactions, such as when accessing the SE email system.

In certain circumstances, where there is a clear business requirement or system limitation, the use of a shared user-ID/password for a group of users or a specific job can be used. Approval by SE ISO and SE management shall be documented in these cases. Additional compensatory controls shall be implemented to ensure accountability is maintained (refer to Information Requirements, Individual Accountability)

Where technically feasible, default administrator accounts shall be renamed, removed or disabled. The default passwords for these accounts shall be changed if the account is retained, even if the account is renamed or disabled.

9. Application Access Control

Access to SE business and systems applications shall be restricted to those individuals who have a business need to access those applications or systems in the performance of their job responsibilities. Access to source code for applications and systems shall be restricted, and these accesses shall be further restricted so that authorized SE staff and contractors can access only those applications and systems they directly support.

10. Monitoring System Access and Use

Systems and applications shall be monitored and analyzed to detect deviation from the access control policy and record events to provide evidence and to reconstruct lost or damaged data. Audit logs recording exceptions and other security-relevant events shall be produced and kept consistent with record retention requirements developed in cooperation with the State Records Management Bureau and SE requirements to assist in future investigations and access control monitoring. Audit logs shall be created and protected.

I. Systems Development and Maintenance Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2010.

Software applications are developed or acquired to provide efficient solutions to SE business problems. These applications generally store, manipulate, retrieve and display information used to conduct SE business. The SE business units become dependent on these applications, and it is essential the data processed by these applications be accurate. It is also critical that the software that performs these activities be protected from unauthorized access or tampering.

To ensure that security is built into all SE information systems, all security requirements, including the need for rollback arrangements, shall be identified during the requirements phase of a project and justified, agreed to and documented as part of the overall business case for an SE information system. To ensure this activity is performed, the SE ISO shall be involved in all phases of the System Development Lifecycle from the requirements definition phase, through implementation and eventual application retirement.

Security requirements and controls shall reflect the business value of the information involved, and the potential business damage that might result from a failure or absence of security measures. This is especially critical for Internet Web and other online applications. The framework for analyzing the security requirements and identifying controls to meet them is associated with threat assessment and risk management which shall be performed by the information owner, reviewed by the SE ISO and written approval by SE executive management

A process shall be established and implemented for each application to:

- address the business risks and develop a profile of the data to help to understand the risks;

- identify security measures based on the risk profile and protection requirements;
- identify and implement specific controls based on security requirements and technical architecture;
- implement a method to test the effectiveness of the security controls;
- identify processes and standards to support changes, ongoing management and to measure compliance.

Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms shall be documented at the application level, SE's Information Systems Security Engineering methodology, and in the SE's security standards documents. The security measures that are implemented shall be based on the threat and risk assessments of the information being processed and cost/benefit analysis.

1. Input Data Validation

An application's input data shall be validated to ensure it is correct and appropriate including the detection of data input errors. Personnel shall be clearly identified to perform these functions. The checks that are performed on the client side shall also be performed at the server to ensure data integrity. Checks shall be performed on the input of business transactions, static data (names, addresses, employee numbers, etc.) and parameter tables. Set up a process to verify and correct fields, characters, completeness of data and range/volume limits.

2. Control of Internal Processing

Data that has been entered correctly can be corrupted by processing errors or through deliberate acts. Checks and balances shall be incorporated into systems to prevent or stop an incorrect program from running. Application design shall ensure that controls are implemented to minimize the risk of processing failures leading to a loss of data or system integrity. Consider the use of correction programs to recover from failures and access to add and delete functions to make changes to application data and to ensure the correct processing of data.

3. Message Integrity

It is necessary to put into place a method to detect unauthorized changes to the content of a transmitted electronic message. Message integrity shall be considered for applications where there is a security requirement to protect the message or data content e.g. electronic funds transfer, EDI transactions, etc. An assessment of threats and risks shall be performed to determine if message integrity is required and to identify the most appropriate method of implementation. It should also be noted that message integrity will not protect against unauthorized disclosure. Encryption techniques are the preferred means of implementing message integrity.

4. Cryptographic Controls

Use of cryptography for protection of high-risk information is preferred when other controls do not provide adequate protection. Encryption is a technique that can be used to protect the confidentiality and integrity of information. Based on a risk assessment, the required level of protection shall be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys employed. To the extent possible, consideration shall also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world. In addition, and to the extent possible, consideration shall be given to controls that apply to the export and import of cryptographic technology.

5. Key Management

Protection of cryptographic keys is essential if cryptographic techniques are used. A secured environment shall be established to protect the cryptographic keys used to encrypt and decrypt information. Access to these keys shall be tightly controlled to only those individuals who have a business need to access the keys. Loss of confidentiality of a cryptographic key would cause all information encrypted with that key to be considered compromised.

6. Protection of System Test Data

Test data is intended to test the expected behavior of software, systems and applications. Test data is developed to test a comprehensive set of conditions and outcomes, including exception processing and error conditions to demonstrate accurate processing and handling of information and the stability of the software, system or application.

Once test data is developed, it shall be protected and controlled for the life of the testing. In those cases where test data is reused, whenever modifications are made to the software, system or application then the test data shall be protected and controlled during the entire useful life. This protection mechanism is essential to ensuring a valid and controlled simulation with predictable outcomes.

Production data may be used for testing only if the following controls are applied;

- a business case is documented, approved in writing by the information owner and access controls, system configurations and logging requirements for the production data are applied to the test environment; or
- a business case is documented, approved in writing by the information owner and personal, sensitive or confidential data shall be masked or overwritten with fictional information and the data shall be deleted as soon as the testing in completed.

7. Information Systems Change Control Procedures

To minimize the possibility of corruption of information systems, strict controls over changes to information systems shall be implemented. Formal change control procedures for business applications shall be developed, implemented and enforced. They shall ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of a system necessary to perform their jobs, and that formal agreement and approval processes for changes are implemented. These change control procedures shall apply to SE business applications as well as systems software used to maintain operating systems, network software, hardware changes, etc.

In addition, access to source code libraries for both SE business applications and operating systems shall be tightly controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

J. Cyber Security Citizens' Notification Requirements

All SEs are required to implement notification procedures in compliance with (any) applicable Federal requirements, contractual requirements, judicial mandates of a qualified court, or State of Montana statutes enacted by the Legislature.

K. Compliance Requirements

The requirements listed in this section shall be in effect beginning Fiscal Year 2009.

1. Monitoring

Consistent with applicable law, employee contracts and SE policies, the SE reserves the right to monitor, inspect, and/or search at any time all SE information systems. Since SE's computers and networks are provided for business purposes, staff members shall have no expectation of privacy in the information stored in or send through these information systems. SE management additionally retains the right to remove from its information systems any unauthorized material.

2. Compliance Reviews

The enterprise IT security office may periodically review compliance by statewide entities to this policy. Such reviews may include, but are not limited to, reviews of the technical and business analyses required to be developed pursuant to this policy, and other project documentation, technologies or systems which are the subject of the published policy or standard.

Compliance with this policy is mandatory. Each user shall understand his/her role and responsibilities regarding information technology security issues and protecting SE's information. The failure to comply with this or any other security policy that results in the compromise of SE information confidentiality, integrity, privacy, and/or availability may result in appropriate action as permitted by law, rule, regulation or negotiated agreement. Each SE shall take every step necessary, including legal and administrative measures, to protect its assets and shall establish the post of SE Information Security Officer to monitor compliance with policy matters.

At the state government entity level, each SE shall implement a process to determine the level of compliance with this policy. A review to ensure compliance with this policy shall be conducted at least annually and SE executive management shall certify and report the SE's level of compliance with this policy in writing to the enterprise IT security office by October 1st of each year. Areas where compliance with the policy requirements is not met shall be documented and a plan shall be developed to address the deficiencies.

SE managers and supervisors shall ensure that all security processes and procedures within their areas of responsibility are followed. In addition, all business units within the SE may be subject to regular reviews to ensure compliance with security policies, standards and procedures.

3. Enforcement and Violation Handling

Any compromise or suspected compromise of this policy shall be reported to the appropriate SE management, the SE Information Security Officer and the enterprise IT security office as required by this policy (refer to Personnel Security Requirements, Security Incident or Malfunctions Management Process). Any violations of security policies may be subject to disciplinary or other appropriate action in accordance with law, rule, regulation, policy or negotiated agreement.

Security incident reports indicating the risk level of the violation shall be reported to responsible entities in accordance with SE labor relations. Access authorization for user accounts involved in a compromise may be suspended during the time when a suspected violation is under investigation. Automated violation reports generated by the various security systems shall be forwarded to the appropriate management and the SE Information Security Officer for timely resolution.

VII. Policy Changes and Exceptions

Changes and exceptions to policies are governed by the Policy for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form.

VIII. Closing

This policy shall be followed unless it conflicts with negotiated labor contracts or specific statutes, which shall take precedence to the extent applicable.

To submit questions or comment on this policy, please e-mail ITpolicy@mt.gov.

Or write to:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700

IX. Cross-Reference Guide

A. Federal/State Laws

- 2-15-114 MCA – Security Responsibilities of Departments for Data.
- 2-17-534 MCA - Security Responsibilities of Department.

B. Policy Documents

- ISO 17799

X. Administrative Use

History Log	
Document ID:	POL-20070522a
Version:	**0.6**
Approved Date:	
Effective Date:	January 1, 2008
Change & Review Contact:	ITpolicy@mt.gov
Review:	Event Review: Any event affecting this architecture paper may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	One year from earliest Effective Date
Last Review/Revision:	
Changes:	